PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-268763
(43)Date of publication of application : 09.10.1998

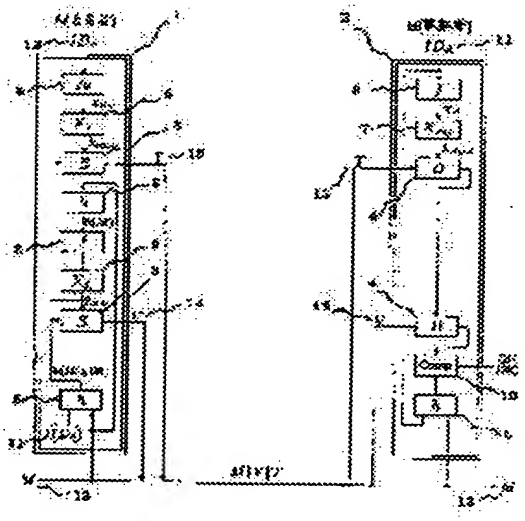
(51)Int.Cl. G09C 1/00
H04L 9/32

(21)Application number : 09-092797
(22)Date of filing : 28.03.1997

(71)Applicant : ADVANCE CO LTD
(72)Inventor : NISHIOKA TAKESHI
IMAI HIDEKI

(54) DIGITAL SIGNATURE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To eliminate authenticator specification and to evade abuse of a signature by separating message signature information and authenticating right information obtained from a message and authenticating the message on the basis of the message signature information and authenticating right information.
SOLUTION: A digital signature of the message consists of message signature information V14 and authenticating right information T15. Then a signature information generating means 1 generates the signature, which is authenticated by using an authenticating means 2,. Namely, an individual identifier IDA11, message signature information V14 obtained from an open message M13, the identifier IDB12 of an opposite person which is made open, and authenticating information T obtained from the open message M13 are generated and outputted in a separated state. An authenticator B certifies whether or not the message has been sent from a legal body by using the obtained open message M13, message signature information V14, authenticating right information T, opposite- person open identifier IDA11.



LEGAL STATUS

[Date of request for examination] 11.03.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Japanese Patent Laid-open Publication No. HEI 10-268763 A

Publication date : October 9, 1998

Applicant : ADVANCE CO LTD

Title : DIGITAL SIGNATURE SYSTEM

[0006]

[Embodiments] According to the present invention, own identifier, message signature information obtained from a public message, a public identifier of the other party, and the authentication right information obtained from the public message are generated and output separately. An authenticating person proves whether the message is delivered from a legitimate person by the obtained public message, the message signature information, the authentication right information, and the other party's public identifier. Fig. 1 depicts a specific example of the present invention.

On the side of a signer, message signature information for authentication and authentication right information is generated by information concerning a key shared with the other party and message information. Namely, on the side of the signer,

• A public message that is a plaintext is converted into key data that can be used as an encryption key. While a converting unit is not particularly limited if it is data corresponding to an

encryption algorithm to which the key is input, a one-way function is preferable because it makes correspondences between inputs and outputs complicated.

• The key information is encrypted based on information shared with the sending end, namely, a shared key, preferably a shared key that is generated corresponding only to the other party's public identifier data. The resultant encrypted information is delivered or transmitted and output, as authentication right information. In addition to be output through ordinary analog or digital communication medium, the information can be recorded in recording medium including FDs (floppy disks), MO disks, CDs, and magnetic tapes and then transmitted.

• Furthermore, public identifier data and data obtained by converting the message in a one-way manner are encrypted by using the key information as a key. The resultant encrypted data is then delivered or transmitted and output, as the message signature information. On the side of an authenticating person,

• A person who proves whether the message is output from a legitimate signer obtains the public message, the message signature information, and the authentication right information.

• A shared key is generated based on the other party's public identifier and the authentication right information is decoded.

• The message signature information is decoded using the decoded

data as a key.

• Furthermore, the other party's identifier and the message data are converted using the aforementioned one-way function.

• The resultant data subjected to one-way function processing is compared to the decoded message signature data. If the data coincides with the message signature data, it is proved that the message is prepared by the legitimate signer. As described above, according to the present invention, the system that an identifier and another party's identifier are input so as to generate a shared key is utilized. Thus, easy handling is realized and anyone can utilize the present invention without special knowledge. It is presupposed that a KPS secret algorithm is obtained from a center authority possessing center algorithms. The KPS secret algorithm and the identifier or the like are based on a so-called KPS system. The system is referred to literatures such as Matsumoto and Imai, "Key Sharing without Communication: KEY PREDISTRIBUTION SYSTEM", Journal of the Institute of Electronics, Information and Communication Engineers, Vol. J71-A, No. 11, pp.2046-2053, Nov. 1998. The present invention includes a plurality of algorithms such as a secret algorithm for signature and a secret algorithm for authentication. The different secret algorithms are obtained by a center algorithm that different identifiers such as a general identifier and a signature identifier are possessed by a center or a plurality of center algorithms corresponding to characters of a plurality of identifiers. The center is configured by an

unmanned or manned device. At least, the center manages center algorithms externally and safely, prepares secret algorithms, and outputs them.

[0007]

[Embodiments] Fig. 1 of the accompanying drawings is a block diagram of the present invention. Reference numeral 1 represents a signature information creating unit that is possessed by a signer and is, for example, a personal computer or a digital computation device such as a digital computation circuit. Particularly, a device with tamper-resistance that internal information is hardly taken out and can be provided in the form of an IC card is preferable as the signature information creating unit. Reference numeral 2 represents an authentication unit that is possessed by an authenticating person and is, like the signature information creating unit 1, for example, a personal computer or a digital computation device such as a digital computation circuit. Also, a device with tamper-resistance that internal information is hardly taken out and can be provided in the form of an IC card is preferable as the authentication unit. When the signature information creating unit 1 and the authentication unit 2 are configured by a personal computer, components that configure the embodiment of the present invention are realized by software such as programs. Reference numeral 3 represents an encryption device that includes an encryption algorithm and converts a plaintext to a ciphertext by input of key data. Examples of the encryption algorithm include,

but are not limited to, DES (Data Encryption Standard) and FEAL cipher (Shimizu, Miyaguchi, and Ohta: "Fast Data Encipherment Algorithm FEAL", Technical Report of the Institute of Electronics, Information and Communication Engineers (Information Theory), VOL.80, No. 113, IT86-33, PP. 1-6, (1986)). Reference numeral 4 represents a decoder that includes a decoding algorithm corresponding to the aforementioned encryption algorithm and converts a ciphertext to a plaintext by input of key data. The same key data is used for the encryption device 3 and the decoder 4. Reference numeral 5 represents a one-way data converting unit that includes a hash function and outputs a single or a plurality of inputs as one-way data. Reference numeral 6 represents a shared key generating unit that generates a shared key that can utilize a shared data generating algorithm described in literatures, such as Blom "Non-Public key Distribution", Advances in Cryptology: Proceedings of CRYPTO '82, Plenum Press, 1983, pp. 231-236. Reference numeral 7 represents an authentication secret key generator with the same structure as that of the shared key generating unit describe above. Reference numeral 8 represents a general ID converter that converts data, which is an assembly of codes and symbols specific to users such as IDs, namely identifiers, for example, data of telephone number and birth date used in ordinary life, in a one-way manner to data that is suitable for input to the subsequently connected secret key generating device. The general ID converter 8 has a structure described in literatures,

such as Matsumoto, Takashima, and Imai, "Portable ID Conversion - Structure of One-Way Algorithm", Technical Report of IEICE, IT89-23, July, 1989. Reference numeral 9 represents a signature ID converter and has the same structure as that of the general ID converter 8. Reference numeral 10 represents a comparator to which a plurality of data are input and which outputs the results of determination such as their match or mismatch. Reference numeral 11 represents a signer's identifier that is, as described above, a code, a symbol, or data that is specific to users and used in a semi-fixed manner, or a combination thereof. The identifier is preferably combined data that is easily handled, such as birth date or telephone number. Reference numeral 12 represents an authenticating person's identifier with the contents described above. Reference numeral 13 represents a message that is data prepared by a signer or existent data. Reference numeral 14 represents message signature information and Reference numeral 15 represents authentication right information.

[0008] An operation of the embodiment of the present invention based on the above structure will be described below. A digital signature of a message is configured by:

[Expression 1] Message signature information V14 and Authentication right information T15.

The digital signature is made by the signature information creating unit 1 and authenticated by the authentication unit 2. The signature

is made by the following process. A message

[Expression 2] M13

is input to the signature information creating unit 1 (a signer is indicated by "A" in this example). The message

[Expression 3] M13

is input together with an identifier

[Expression 4] IDA 11

of the signer A, to the one-way data converting unit

[Expression 5] h5.

An output of the one-way data converting unit, namely, an authenticator

[Expression 6] h(IDA||M)

is input to the encryption device

[Expression 7] E3

and encrypted using a message-specific key

[Expression 8] KAM,

so that message signature information

[Expression 9] V14:

[Expression 10]V=EKAM(h(IDA||M))

is generated. Next, a description will be given of generation of the message-specific key

[Expression 11] KAM. The message

[Expression 12] M13

is input to the one-way data converting unit

[Expression 13] h5.

An output

[Expression 14] h(M)

of the one-way data converting unit is input to the general ID converter

[Expression 16] f8

that converts the output so as to have a format to be input to the signer's shared key generating unit

[Expression 15] XA6

(for example, a secret algorithm for Key Predistribution System (KPS)). The message-specific key is obtained by inputting the output of the general ID converter to the signer's shared key generating unit

[Expression 17] XA6,

and the output result is

[Expression 18] KAM.

Generation of the authentication right information

[Expression 19] T

is described below. An identifier

[Expression 20] IDB 12

of an authenticating person (indicated by "B" in this example) is input to the signature information creating unit 1. The identifier

[Expression 21] IDB 12

of the authenticating person is input to the signature ID converter

[Expression 22] fV9.

An output of the ID converter is input to the signer's shared key generating unit

[Expression 23] XA6,

so that a signature key

[Expression 24] kABV

is generated. The message-specific key

[Expression 25] kAM

is input to the encryption device

[Expression 26] E3,

and encrypted using the signature key

[Expression 27] kABV.

Accordingly, the authentication right information

[Expression 28] T15:

[Expression 29] T=EkABV(KAM)

is generated. The message

[Expression 30] M13,

the message signature information

[Expression 31] V14,

and the authentication right information

[Expression 32] T15

are sent to the authenticating person. Authentication of the digital signature is performed by the following process. The authenticating person inputs the identifier

[Expression 33] IDA11

of the signer to the authentication unit 2. The identifier

[Expression 34] IDA11

is input to the general ID converter

[Expression 35] f8.

An output of the general ID converter is input to the authentication secret key generating unit, and an authentication key

[Expression 36] kBVA

is output. The authentication key

[Expression 37] kBVA

is subjected to only a decoding processing because of the tamper-resistance of the authentication unit 2. The authentication right information

[Expression 38] T15

input to the authentication unit 2 is input to the decoder

[Expression 39] D4,

and decoded using the authentication key,

[Expression 40] kBVA

so that the message-specific key

[Expression 41] kAM

is decoded. The message signature

[Expression 42] V14

input to the authentication unit 2 is input to the decoder

[Expression 43] D4,

and decoded using the message-specific key

[Expression 44] KAM.

Accordingly, a decoded authenticator

[Expression 45] DKAM(V)

is output. On the other hand, the message

[Expression 46] M13

is also input to the authentication unit 2, together with the signer's identifier

[Expression 47] IDA11,

to the one-way data converting unit

[Expression 48] h5,

so that an authenticator

[Expression 49] h(IDA||M)

is generated. The decoded authenticator

[Expression 50] DKAM(V)

and the generated authenticator

[Expression 51] h(IDA||M)

are input to a comparator Comp 10. If they coincide with each other, "OK" is output. On the other hand, if they do not coincide with

each other, "NG" is output. According to the embodiment, although the message signature information

[Expression 52] V14

and the authentication right information

[Expression 53] T15

are generated at one time, a signer can generate only new authentication right information

[Expression 54] T'

from a message

[Expression 55] M13

and a new identifier

[Expression 56] IDB'.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－268763

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ａ
			６４０Ｄ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ

審査請求　未請求　請求項の数３　ＦＤ　（全 ７ 頁）

(21)出願番号　特願平9－92797

(22)出願日　平成９年(1997)３月28日

特許法第30条第１項適用申請有り　1997年１月29日～２月１日　開催の「ＳＣＩＳ'97 The 1997 Symposlum on cryptography and Information Security」において文書をもって発表

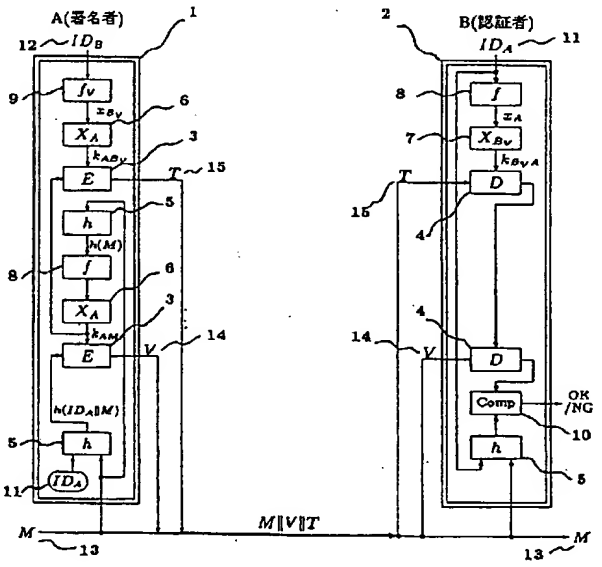
(71)出願人　000126757
株式会社アドバンス
東京都中央区日本橋小舟町５番７号

(72)発明者　西岡　毅
神奈川県相模原市淵野辺２丁目19番１号

(72)発明者　今井　秀樹
神奈川県横浜市六ツ川３丁目76番３号　横浜パークタウンＪ－902

(54)【発明の名称】　デジタル署名方式

(57)【要約】
【課題】従来の署名方式で問題であった、1つの署名に対して認証者が1人に特定されてしまう、1つの耐タンパーモジュールが破られるだけですべての署名の有効性が喪失してしまう等問題点を解消するデジタル署名方式を提供する。
【解決手段】自分の識別子と、公開メッセージにより得られたメッセージ署名情報と、相手の公開された識別子と公開メッセージより得られた認証権情報を分離した状態で生成出力し、認証者は、入手した公開メッセージ、メッセージ署名情報、認証権情報と相手公開識別子により、このメッセージが正当な者から発信されたものであるかどうかを証明可能とする。



1

【特許請求の範囲】

【請求項1】 メッセージより得られるメッセージ署名情報及び認証権情報を分離した状態とし、前記メッセージ署名情報、認証権情報に基づきメッセージの認証を行うデジタル署名方式。

【請求項2】メッセージ署名情報生成に使用する暗号化鍵がメッセージ固有であることを特徴とする請求項１に記載のデジタル署名方式。

【請求項3】認証権情報生成に使用する暗号化鍵が認証者毎に固有であることを特徴とする請求項１に記載のデジタル署名方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、共通鍵暗号と耐タンパーモジュールを利用したIDに基づく暗号システムにおける、デジタル署名に関する。

【０００２】

【従来の技術】従来のこのタイプの署名方式は、認証者間における認証用（復号）鍵の共有の仕方で2つに大別される。1つはそれぞれの署名者認証者間で固有の鍵を用いる方式。この場合、1つの署名に対して認証者が1人に特定されてしまう点が問題である。もう1つは認証者が認証用鍵を共有する方式、この場合は、認証者が特定されないが、1つの耐タンパーモジュールが破られるだけですべての署名の有効性が喪失してしまう点が問題である。

【０００３】

【発明が解決しようとする課題】この発明は、上記した問題点を解消するデジタル署名方式を提供することを目的とする。

【０００４】

【課題を解決するための手段】上記目的を達成するため、この発明の署名方式は、メッセージの正当性を担保するメッセージ署名と認証者がその正当性を確認できる認証権を分離した署名であることを特徴とする。メッセージ署名情報に用いる暗号化鍵は、署名者固有だけでなく、メッセージにも固有であることを特徴とする。認証権情報に用いる暗号化鍵は署名者認証者間で固有な鍵を用いることを特徴とする。認証権情報とは、内容は異なるが、同種の処理能力を有するグループに属している者が、所有することができるものであり、本願発明では、例えば、センタ等グループを管理するものが各エンテイテイに付与する。

【０００５】

【作用】この発明のデジタル署名方式は、署名と認証権が分離しているから、署名部分の共通性により、デジタル署名の同一性が図れ認証者の特定がされない。署名にメッセージ固有な暗号化鍵を用いることにより、認証権の乱用が避けられ、耐タンパーモジュールが破られても、署名の偽造が判別できる。認証権に認証者毎に固有な暗号化鍵を用いることにより、高々数個の耐タンパーモジュールが破られても署名の有効性は失われない。耐タンパー性とは、ＩＣカードのように、入出力端及び必要最小限の電気的接続部を表出した以外は、電気回路が樹脂等で封入された担体等で実現されたものであり、当該封入を破ってもその内容を見ることが非常に困難なものである。尚、耐タンパー性については、今井秀樹「暗号のおはなし」（財）日本規格協会(1993)pp. 81等の公知文献に記載が参照される。

2

【０００６】

【実施の形態】本発明は、自分の識別子と、公開メッセージにより得られたメッセージ署名情報と、相手の公開された識別子と公開メッセージより得られた認証権情報を分離した状態で生成出力し、認証者は、入手した公開メッセージ、メッセージ署名情報、認証権情報と相手公開識別子により、このメッセージが正当な者から発信されたものであるかどうかを証明可能とするものであって、図１にその具体的１実施例を示す。

署名者側において

証明用のメッセージ署名情報及び認証権情報を、相手との共有鍵情報及びメッセージ情報から作成するものである。即ち、署名者側において、

・平文化された主に公開されるメッセージに対し、メッセージを暗号化鍵として使用可能な鍵データに変換する。その変換手段としては、鍵を入力する暗号アルゴリズムに対応するデータであれば特に限定されないが、１方向性を有する関数が入出力の対応関係を複雑化する点で好ましいものである。

・この鍵情報を、送り側と共有可能な情報、即ち共有鍵、好ましくは相手の公開された識別子データにのみ対応して生成される共有鍵に基づいて暗号化し、これを認証権情報として配送又は伝送等して出力する。この出力は一般のアナログ、デジタル通信媒体を使用して伝送することの他、ＦＤ（フロッピーデイスク）、MOデイスク、ＣＤ、磁気テープ等の記録媒体に記録配送すること等を例示するものである。

・更にこの鍵情報を鍵とし、自己の公開された識別子データとメッセージを一方向的に変換したデータをこの鍵を用いて暗号化してメッセージ署名情報として配送又は伝送などして出力する。認証者側において、

・このメッセージが正当な署名者から出力されているものであるかを証明する者は公開されたメッセージとメッセージ署名情報、認証権情報を入手する。

・相手の公開された識別子に基づいて共有鍵を生成し、認証権情報を復号する。

・この復号したデータを鍵として、メッセージ署名情報を復号する。

・更に、相手識別子と、メッセージデータを上述と同様の一方向性関数により処理変換する。

・この一方向関数処理したデータと復号したメッセージ

3

署名データを比較し、一致すれば、正当な署名者が作成したメッセージであることが証明できる。上述した様に本発明では、相手識別子及び自分の識別子を入力して共有鍵を生成する手段が採られ、このことにより、取り扱いを容易にし、誰でもが特殊な知識を要せず利用可能とするものであるが、その際、センタアルゴリズムを所有するセンタ機関からＫＰＳ秘密アルゴリズムを取得することを前提とする。ＫＰＳ秘密アルゴリズム、識別子等は、いわゆるＫＰＳ方式に基づくものであるが、この方式については、松本、今井、”暗号化鍵を通信なしで共有する方法：ＫＥＹ　ＰＲＥＤＩＳＴＲＩＢＵＴＩＯＮ　ＳＹＳＴＥＭ，”信学論　Vol. J71-A, No. 11 pp. 2046-2053, Nov. 1988.　などの文献に示されるものが参照される。ところで、本願発明は、署名用秘密アルゴリズム及び認証用秘密アルゴリズム等の複数のアルゴリズムを具備するものであるが当該異なる秘密アルゴリズムは、それぞれ、汎用識別子、署名用識別子といった異なる識別子をセンタが所有する一つのセンタアルゴリズム、或いは複数の識別子の性格に対応した複数のセンタアルゴリズムに施すことにより得られるものであれば足りるものである。尚、センタは、無人駆動乃至有人駆動される装置等で構成されるものであり、少なくとも、対外的にセンタアルゴリズムを安全に管理でき秘密アルゴリズムを作成出力するものであればよい。

【０００７】

【実施例】添付図面で図1は本発明のブロック図である。１は、署名情報作成手段であり、署名する者が所有する、パーソナルコンピュータ、デジタル演算回路等のデジタル演算装置が例示されるが、特にＩＣカード等の形態可能で、内部情報を取りにくい耐タンパー性を有する装置が好ましい。２は、認証手段であり、認証する者が所有するものであって、署名情報作成手段１と同様、パーソナルコンピュータ、デジタル演算回路等のデジタル演算装置が例示されるが、特にＩＣカード等の形態可能で、内部情報を取りにくい耐タンパー性を有する装置が好ましい。署名情報生成手段１及び認証手段２は、パーソナルコンピュータによって構成される場合は、以下の本発明の実施例を構成する各構成要件は、プログラム等のソフトウエアで実現されるものである。３は、暗号器であり、暗号アルゴリズムを内蔵し、鍵データの入力により、平文を暗号文に変換するものである。この暗号アルゴリズムは、例えば、ＤＥＳ (Data Encryption Standard)、ＦＥＡＬ暗号（清水、宮口、太田：”高速データ暗号アルゴリズムＦＥＡＬ”、電子通信学会技術報告、（情報論）、VOL. 80, No. 113, IT86-33, PP. 1-6, (1986年)）等が例示されるがこれに限定されるものではない。４は、復号器であり、上記暗号アルゴリズムに対応した復号アルゴリズムを内蔵し、鍵データの入力により、暗号文を平文に変換するためのものである。暗号器３、復号器４に使用される鍵データは、同一の鍵データ

4

が使用される。５は、一方向データ変換手段であり、ハッシュ関数等を内蔵し、単数乃至複数の入力を一つの一方向データとして出力するものである。６は、共有鍵生成手段であり、共有鍵を生成する手段であって、例えばＢｌｏｍ”Non-Public key Distribution,” Advances in Cryptology : Proceedings of CRYPTO'82 , Plenum Press, 1983, pp. 231-236等の文献に記載された共有データ生成アルゴリズムも利用できる。７は、認証用秘密鍵生成器であり、上述した共有鍵生成手段と同様の構成を有する。８は、汎用ＩＤ変換器であり、ＩＤ即ち識別子等、本人固有の符号、記号等の集合体であり、通常生活で使用される電話番号、生年月日等のデータを、一方向的に変換し、後段に接続される秘密鍵生成器の入力に適したデータに変換するものである。この汎用ＩＤ変換器８は、具体的には、松本、高嶋、今井”簡易型ＩＤ変換一方向性アルゴリズムの構成”信学技報　ＩＴ８９－２３，July　１９８９）の文献に記載された構成をとるものである。９は、署名用ＩＤ変換器であり、汎用ＩＤ変換器８と同様の構成を有する。１０は、比較照合器であり、複数のデータを入力し、これらのデータを比較し、その一致、不一致を判定した旨を出力するものである。１１は、署名者識別子であり、上述した様に本人固有で半固定的に用いられる符号、記号、データ及びこれらの組み合わせであって、生年月日、電話番号等取り扱い上容易な組み合わせデータが好ましい。１２は、認証者の識別子であって、上述のような内容の識別子である。１３は、メッセージであり、署名者が作成した或いは既成のデータである。１４は、メッセージ署名情報であり、１５は、認証権情報である。

【０００８】以上の構成に基づく本発明の実施例の動作を以下に示す。メッセージのデジタル署名は

【数１】

$$\text{メッセージ署名情報 } V_{14},\ \text{認証権情報 } T_{15}$$

から構成される。署名情報作成手段1で署名され、認証手段２を使って認証される。署名は以下の手順でなされる。署名情報作成手段１（当例の署名者はＡとする）にメッセージ

【数２】

$$M_{13}$$

を入力する。このメッセージ

【数３】

$$M_{13}$$

は署名者Ａの識別子

【数４】

$$ID_{A\ 11}$$

とともに一方向データ変換手段

【数５】

$$h_5$$

に入力される。この出力、認証子

5

【数６】

$$h(ID_A \| M)$$

が暗号器

【数７】

$$E_3$$

に入力され、メッセージ固有な鍵

【数８】

$$k_{AM}$$

でもって暗号化され、メッセージ署名情報

【数９】

$$V_{14}:$$

【数１０】

$$V = E_{k_{AM}}(h(ID_A \| M))$$

が生成される。次に、メッセージ固有な鍵

【数１１】

$$k_{AM}$$

の生成を示す。メッセージ

【数１２】

$$M_{13}$$

は一方向データ変換手段

【数１３】

$$h_5$$

に入力される。この出力

【数１４】

$$h(M)$$

を署名者の共有鍵生成手段

【数１５】

$$X_A 6$$

（例えば、Key Predistribution System, KPSの秘密アルゴリズム）に入力できる形式に変換する汎用ID変換器

【数１６】

$$f_8$$

に入力する。この出力を署名者の共有鍵生成手段

【数１７】

$$X_A 6$$

に入力した出力結果が

【数１８】

$$k_{AM}$$

である。認証権情報

【数１９】

$$T$$

の生成を以下に示す。認証者（当例ではＢとする）の識別子

【数２０】

$$ID_B 12$$

を署名情報作成手段１に入力する．認証者の識別子

【数２１】

$$ID_B 12$$

は署名用ID変換器

6

【数２２】

$$f_V 9$$

に入力される。この出力を署名者の共有鍵生成手段

【数２３】

$$X_A 6$$

に入力して署名用鍵

【数２４】

$$k_{ABV}$$

が生成される。メッセージ固有な鍵

【数２５】

$$k_{AM}$$

を暗号器

【数２６】

$$E_3$$

に入力し、この署名鍵

【数２７】

$$k_{ABV}$$

でもって暗号化することで認証権情報

【数２８】

$$T_{15}:$$

【数２９】

$$T = E_{k_{ABV}}(k_{AM})$$

が生成される。メッセージ

【数３０】

$$M_{13}$$

とメッセージ署名情報

【数３１】

$$V_{14}$$

と認証権情報

【数３２】

$$T_{15}$$

を併せて認証者に送る。このデジタル署名の認証は以下の手順でなされる。認証者は、署名者の識別子

【数３３】

$$ID_A 11$$

を認証手段２に入力する。識別子

【数３４】

$$ID_A 11$$

は汎用ＩＤ変換器

【数３５】

$$f_8$$

に入力される。この出力が認証用秘密鍵生成器に入力されると、認証用鍵

【数３６】

$$k_{BVA}$$

が出力される。この認証用鍵

【数３７】

$$k_{BVA}$$

は、認証手段２の耐タンパー性により復号処理しかでき

7

ない。認証権情報
【数３８】
T 15
を認証手段２に入力すると、復号器
【数３９】
D_4
に入力され、認証用鍵
【数４０】
k_{BvA}
を用いて復号すると、メッセージ固有な鍵
【数４１】
k_{AM}
が復号される。メッセージ署名
【数４２】
V 14
を認証手段２に入力すると、復号器
【数４３】
D_4
に入力され、メッセージ固有な鍵
【数４４】
k_{AM}
により復号すると、復号された認証子
【数４５】
$D_{k_{AM}}(V)$
が出力される。一方、メッセージ
【数４６】
M 13
も認証手段２に入力され、署名者の識別子
【数４７】
ID_A 11
とともに、一方向データ変換手段
【数４８】
h 5
に入力されると、認証子
【数４９】
$h(ID_A \| M)$
が生成される。この復号された認証子
【数５０】
$D_{k_{AM}}(V)$
と生成された認証子
【数５１】
$h(ID_A \| M)$
が比較照合器 Comp 10に入力され、一致すればOKが、不一致のときはＮＧが出力される。以上の実施例では、メッセージ署名情報
【数５２】
V 14
と認証権情報
【数５３】
T 15

8

の双方を一度に生成したが、署名者側は新たな認証権情報
【数５４】
T'
だけをメッセージ
【数５５】
M 13
と新たな識別子
【数５６】
$ID_{B'}$
とから生成することも可能である。
【０００９】本実施例においては、各鍵変換器が内蔵するアルゴリズムが異なる複数のアルゴリズムを必要とすることから、このアルゴリズムをメモリに記録する必要があるが、ＩＣカード等その容量が限られている場合に好適なアルゴリズムの構成例を以下に説明する。
メモリ効率
上述の如く、複数の鍵共有の為の秘密アルゴリズムを納めなければならない。これは少なくとも2つの問題点を提議する。必要なメモリ量が2倍になること、実質的な結託閾値が1/2になることである。以下、この点について考察する。現方式について、次のような4つの鍵を有している:
【数５７】

1. k_{AB} ：守秘用
2. k_{ABv} ：署名用
3. k_{A_vB} ：認証用
4. $k_{A_vB_v}$

このうち、4番目の鍵は使用していない。そこで、この鍵を削除するようなセンタアルゴリズム（center-algorithm），秘密アルゴリズム（secret-algorithm）の構成法を考察する。
【００１０】Grand ID-vector
識別子
【数５８】
ID_A
から2つのID-vectorを準備していたが:
【数５９】
x_A^i：汎用ＩＤ-vector.

x_{Av}^i：認証用ＩＤ-vector.

これを1つに統合する。
【数６０】
$$\tilde{x}_A = \begin{pmatrix} x_A \\ x_{Av} \end{pmatrix}$$

9

・・・・・・（1）

これは、

【数６１】

$$\tilde{x}'_A = x'_A \ (i=1,\ldots,m), \quad \tilde{x}^{m+i}_A = x'_{Av} \ (i=1,\ldots,m)$$

をまとめたものである。

【００１１】Grand secret-algorithm

このID-vectorに基づき、center-algorithmを拡大する、

【数６２】

$$\tilde{G} = \begin{pmatrix} G & G_V \\ G_V & O \end{pmatrix},$$

・・・・・・・・（2）

ここで、

【数６３】

$$G,\ G_V$$

はサイズ（ｍ×ｍ）のsymmetric matrixである。不要な鍵を省くような構造を導入した。従って、総サイズは（２ｍ×２ｍ）であるが。正味のメモリ量は２m2ｈ－bitである。ここでｈは鍵の長さである。

【００１２】Grand secret-algorithm

以上から、秘密アルゴリズム（secret-algorithm）も拡大される，

【数６４】

$$\tilde{X}_A = ({}^t x_A G + {}^t x_{Av} G_V,\ {}^t x_A G_V).$$

このGrand secret-algorithmを基にして、2つのsecret-algorithmを導く。

汎用secret-algorithm:

【数６５】

$$X_A \equiv \tilde{X}_A(x_{Av} = 0) = ({}^t x_A G,\ {}^t x_A G_V)$$

・・・・（3）

このサイズは（１×２ｍ），メモリ量は２ｍｈ-bitである。

認証用secret-algorithm:

【数６６】

$$X_{Av} \equiv \tilde{X}_A(x_A = 0) = ({}^t x_{Av} G_V,\ 0)$$

・・・・（4）

このサイズは（１×２ｍ），正味のメモリ量はｍｈ－bitである。このように構成することで、

【数６７】

$$k_{AvBv} = 0$$

とすることができる。一方、secret-algorithmの総メモリ量は正味３ｍｈ-bitである。これはメモリ量が基本型に比して見かけ上は1.5倍になっているようにみえる。しかし、結託閾値を考慮すると、基本型の実効結託閾値

10

がｍ／２なので、同じ安全性強度で比較すると、メモリ量は３／４倍に改善されていることになる。

【００１３】上述したメモリ効率の動作は、センタにおいて秘密アルゴリズムを生成出力する際のものである。即ち、秘密アルゴリズムを入手し、センタにより管理されるグループに入ろうとするものが、任意に汎用及び署名用のを識別子を選択作成し、センタに送付する。センタは、これら識別子を、（１）式に基づいた形式に変換し、（２）式に基づくセンタアルゴリズムを実行する演算手段に入力する。センタは、この演算手段で実行して得られた（３）式、（４）式で示す秘密アルゴリズムをグループに入ろうとするものに、送付する。送付の際、これら秘密アルゴリズムは、その性質上秘密であることが条件であることから、上述した耐タンパーモジュールに記憶させた状態、或いは、これら暗号化したプログラムとしてフロッピーデイスク、ＣＤ、光磁気デイスクに記録した状態が例示される。尚、上述した通り、秘密アルゴリズム実効ルーチンの他、図１で示す動作を行う汎用プログラムを併せて送付する場合もある。

【００１４】

【発明の効果】この発明のデジタル署名方式は、共通鍵暗号に基づくので、処理速度とデータ量の大きさという効率性の点で公開鍵暗号に基づくデジタル署名方式より優れている。メッセージ署名と認証権が分離しているので、認証者特定性はない。その上、署名の乱用が避けられる。特に非公開性のある情報に対して署名者の権利を保護できる署名である。認証者固有、メッセージ固有な暗号化鍵をもちいた署名なので、高々数個の耐タンパーモジュールが破られても署名の有効性が喪失しない堅牢性を備えている。

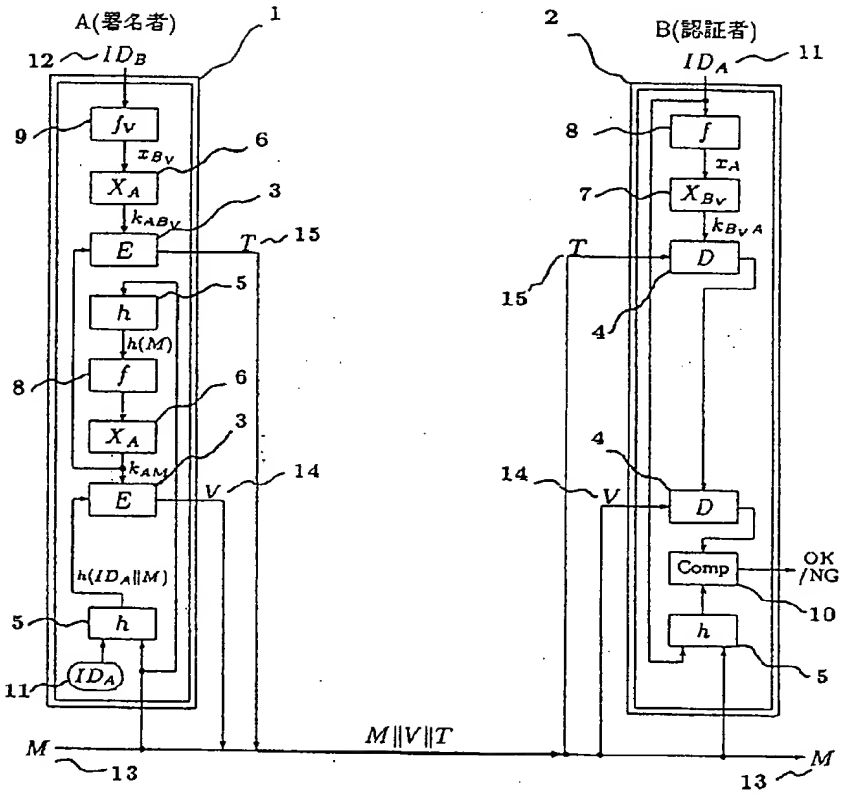
【図面の簡単な説明】

【図１】本発明のブロック図である。

【符号の説明】

１　署名情報作成手段
２　認証手段
３　暗号器
４　復号器
５　一方向データ変換手段
６　共有鍵生成手段
７　認証用秘密鍵生成器
８　汎用ID変換器
９　署名用用ID変換器
１０　比較照合器
１１　署名者の識別子
１２　認証者の識別子
１３　メッセージ
１４　メッセージ署名情報
１５　認証権情報

【図１】


A(署名者)
B(認証者)
ID_B
ID_A
f_V
x_{BV}
X_A
k_{ABV}
E
h
h(M)
f
k_{AM}
$h(ID_A \| M)$
ID_A
$M \| V \| T$
M
T
V
f
x_A
X_{BV}
$k_{BV A}$
D
Comp
OK
/NG
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15